Cyber Security Summit – Working group 4

Cyber defense is becoming a business-critical core skill

Major international companies are subjected to an increasing number of cyber attacks which target their entire value-added chain. The highly professional attackers are characterized by a procedure based largely on a division of labor, and they hit a wide variety of points within the supply chain.

Extremely well-disguised, they operated in secret for weeks and months, as one of the participants in the working party reported. Gradually they gained access to the key know-how which distinguished the attacked companies from their competitors. Since such attacks, known as Advanced Persistent Threats (APT), endangered the companies' market positions, they were at the top of the agenda for those responsible for security.

Building recognition-based defense mechanisms
Within the closed framework of their discussion group and its distinguished members, a number of participants reported from large industrial corporations on attacks on the crown jewels of their businesses. Due to the high degree of professionalism of the attackers, the security experts again and again had found it extremely difficult to detect the incidents quickly. Those affected regarded their still too event-driven protection plans as obstacle number one. Anyone who had first to measure security incidents before he could defend himself against them was at a disadvantage for too long, particularly against APT attacks.

Things were made more difficult because the vulnerable areas in the value-added chains were dramatically increasing in number. The working party participants went into particular detail on the Internet of Things, the triumph of mobile devices and the way social networks were becoming harder and harder to control. Traditional, i.e., purely reactive protection plans were more and more frequently meeting their limits. Against this background, the working group for the development of recognition-based security models agreed to collect all the relevant information and make it available for evaluation in real time. In order to restore arms parity with the attackers, companies needed to be able to examine their entire data traffic for abnormalities in real time. The working group participants agreed that such an analytical perspective could only be achieved by constructing an appropriately powerful Big Data environment.

Cyber security has reached the boardroom

In view of the serious increase in risks, cyber defense capability has developed into a key entrepreneurial skill. It was the unanimous view of the industrial representatives present that this required intensive cooperation in the ITC area and the areas of Corporate Governance and Corporate Risk Management. And the subject of cyber security had now become firmly established in boardrooms. In view of the major penetration of added value with Internet systems, top management had recognized that a large number of business risks were now very closely interwoven with cyber security risks.

Nevertheless, some of the CIOs present stated that considerable efforts would still be required to ensure that the requisite investment budgets for the impending reconstruction of security systems would be made available. In this context, participants from the chemical industry pointed out that they had found it much easier to have the desired funds released once they had learned to formulate their investment projects exclusively in the language of their sector. Previously they had relied too much on a purely IT-based argument, to which the ears of top management had evidently not been accustomed.

Support from the world of politics

When the discussion came round to the role of the political world, considerable skepticism emerged among the participants. The industry representatives present unanimously demanded standardized "norms of behavior" at the international level. However, there was a consensus within the group that such an agreement was very unlikely in the foreseeable future. Even when considering their own national governments, the participants voiced serious doubts as to whether the politicians were capable of acting with sufficient speed against the changing and growing cyber threats.

It was all the more important to bundle economic strength to an even greater extent than before. Even large corporations now needed assistance in handling on their own the many different threats that had emerged. In order to stay on the same level as the highly qualified attackers, cooperation would have to be strengthened, especially at the staffing level. It was also necessary to find effective solutions for the area of the SMEs, which were assuming a key role in the supply chains of a number of sectors, but which lacked the resources required for effective cyber security. Thus an increase in knowledge transfer to the suppliers' area was essential.

In this context, discussion participants from vehicle construction, arms technology and the process industry agreed to network the expertise of their Security Operation Centers (SOCs) and Computer Emergency Response Teams (CERTs) in a sector-specific way. Only then

could effective solutions be found which would take sufficient account of the business processes and threat patterns of their sectors. In addition, there were excessive differences in the readiness to tolerate a particular degree of risks. Therefore sector-specific alliances were much better able to achieve the optimum degree of cyber security.